Notice of Allowability	Application No.	Applicant(s)	
	09/854,493	WOLFF ET AL.	
	Examiner	Art Unit	
	Thomas M. Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *11/21/05*.

2. ☒ The allowed claim(s) is/are *1-4,10-13 and 19-22*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

1. Claims 1-4, 10-13, 19-22 are pending.

2. Claims 5-9, 14-18, 23-27 have been canceled.

Reasons for Allowance

3. Applicant has amended independent claims 1, 10, 19 to further recite the limitations

In reference to claim 1:

Dyson (Column 4, lines 10-25) discloses a computer program product comprising a computer program operable to control a computer to detect a malicious alteration to a stored computer file, said computer program comprising:

- File comparing logic operable to compare said stored computer file with an archive copy of said computer file stored when said stored computer file was created(Figure 2, step 4) & (Column 5, lines 5-8) & (Column 4, lines 10-25)
- Comparison response logic operable if said file comparing logic detects that said stored computer file and said archive computer file do not match to trigger further countermeasures against a potential malicious alteration. (Column 4, lines 10-25)
- Wherein a subset of file types stored by said computer are subject to comparison by said file comparing logic and to creation of an archive copy for use with said file comparing logic. (Column 2, line 57 – Column 3, line 10):
- Wherein said archive copy of said stored computer file is created for a subset of file types stored by said computer; (Column 2, line 57 – Column 3, line 10):

- Wherein said subset of file types includes one or more of :
- Executable file types; (Column 2, line 62)
    - Dynamic link library file types; (Column 3, lines 4-6)

Dyson fails to disclose an embodiment where the entire contents of one file are compared with the contents of another file. Dyson rather, discloses a comparison being performed based on the hash IDs.

However, as Dyson discloses, the motivation behind comparing the identifiers of the two files is specifically to determine whether or not the files are identical or whether or there is an attribute to distinguish the file. For example, Dyson, Column 4, lines 10-20 recite : Step 7 shows comparing the first and second identifiers to identify a possible match that would verify the integrity of the second file, that is the contents of the second file are identical with the contents of the previous first file. "

Jamsa "Comparing two files with COMP" (pgs. 392-401, 406-407) discloses a method of comparing two files exactly by comparing the contents byte for byte.

Jamsa "Comparing files with FC" (pgs. 392-401, 406-407) yet again discloses a method of comparing the contents of two files exactly byte for byte provided that the switch /B is used with the command.

Jamsa, pg 393 2nd paragraph discloses that COMP(the version described by Jamsa) provides the advantage of being user friendly.

It would have been obvious to one of ordinary skill in the art at the time of invention to directly compare the entire contents of the stored computer files using the COMP utility to determine file alteration in order to provide a means that is more user friendly.

However, neither Dyson nor Jamsa discloses

Wherein upon, creation of said stored computer file, said archive copy of said computer file is also created; (Column 3, lines 57-68)

Dyson rather discloses that the stored computer file, the first file, is archived at a remote location, and at some point later, the unverified second file is retrieved. (Column 3, lines 63-67)

It is specifically noted that Dyson' "second file" is most directly an older version of the first file, "created" or coming into existence when the file is to be verified.

Applicant's claim 1 claims the creation of an archived copy upon the creation of the first file. Dyson by contrast, stores the first file in a remote location. At some point in the future when the integrity of that file is verified, it is referred to as a second file, due to its dubious status as an unverified file. (Column 3, lines 63-67) The file gains the dubious

file status by the passage of time, or being placed on an unsecure server, or presumably any means by which the question of the integrity of the file has been raised to the degree so that it warrants a necessity to verify its contents. As previously stated, at this point, Dyson refers to this file as an "unverified second file" (Column 3, lines 63-67).

Because Dyson seeks to verify this "unverified second file" for its execution, (Column 4, lines 20-25), the Examiner has considered this file to be the "stored computer file" in Claim 1, while considering the first file or modification thereof, stored locally on Dyson to be the "archived file" of claim 1.

In this sense, this is the closest recitation to the limitations of claim 1 that Dyson and Jamsa present. Dyson, upon creation of the said stored computer file (saved remotely), also stores the archived file.(stored locally)

However, this combination of Dyson and Jamsa remains deficient. As the Examiner noted above, Dyson does not actually store the first file or archived file on the local computer. Instead Dyson clearly stores a hash of the file. Furthermore, while Jamsa recites reasons why it would be advantageous to use the COMP or FC file comparing utilities, it lends no actual motivation or recitation to modify Dyson to use the entire file locally rather than create a hash of the file locally.

It is the Examiner's position that if a modification to Dyson could be made in which the actual files are stored and compared rather than identifiers, such a modification would read upon Applicant's claims.

A search of the prior art has not uncovered motivation or recitation which would call for the deconstruction of Dyson as such. Accordingly, the rejections to claim 1 are withdrawn, and claim 1 is allowable.

Claims 10 and 19 are substantially similar to claim 1 and are allowable for the same reasons.

Claims 2-4, 11-13, 20-22 are dependent claims which depend on allowable claims 1, 10, and 19 respectively and are allowable because their independent claims are allowable.

Conclusion

4. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571)272-3838.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 571-273-8300
Customer Service Representative	Telephone: 571-272-2100	Fax: 571-273-8300

TMH

Feburary 17th, 2006

E. Moise

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER